ISOO A6(?)

DRAFT
11 JUN
~~8 MAY~~ 1979

MEMORANDUM FOR: Assistant for Information, DDA

STATINTL FROM : [redacted]
Agency Security Classification Officer, ISAS

SUBJECT : Executive Order 12065: Access by the Information Security Oversight Office to CIA Information

1. You have requested comments regarding the authority of the Information Security Oversight Office (ISOO) to gain access to CIA information and the responsibility of the Agency to furnish or deny such access. You also have requested views regarding an actual request for such access in an ISOO letter dated 12 April 1979. The following is essentially a summary of responsibilities relating to access, and a recommended approach to working with ISOO in a spirit of cooperation consistent with these responsibilities.

2. The information to which ISOO should have access is that information which is "necessary to fulfill" ISOO responsibilities pursuant to the Order (Sections 5-502(h) and 5-405). Therefore, determining ISOO's access authority requires that we first determine the extent of ISOO's responsibilities:

a. Section 5-201 of the Order specifies in part that the Administrator of General Services shall delegate to ISOO his responsibility for "implementing and monitoring the program established pursuant to this Order".

b. Section 5-202 specifies in part that the Director, ISOO shall:

(1) oversee agency actions to ensure compliance with the Order and implementing directives;

(2) consider and take action on complaints and suggestions with respect to the administration of the information security program;

SUBJECT: Executive Order 12065: Access by the Information Security Oversight Office to CIA Information

(3) exercise the authority to require that information he determines is classified in violation of the Order be declassified, subject to agency appeal to the National Security Council (NSC);

(4) develop implementing directives, in consultation with the agencies, and promulgate them, subject to NSC approval;

(5) review all agency implementing regulations and agency guidelines for systematic declassification review and require changes where not consistent with the Order or implementing directives, subject to agency appeal to NSC.

c. Section 5-202(h) specifies that the Director, ISOO shall have the authority to conduct on-site reviews of the information security program of each agency and to require such reports, information, and other cooperation as necessary to fulfill his responsibilities. If such reports, inspection, or access to specific categories of classified information would pose an "exceptional national security risk," the agency head may deny access, subject to Director, ISOO appeal to NSC.

d. Section 4-204 specifies, in regard to the "system of accounting for special access programs" established and maintained by each agency head, that the Director, ISOO shall have "non-delegable access to all such accountings."

3. ISOO responsibilities thus are cast by the Order primarily in terms of overseeing agency program implementation and requiring information about such programs. Authority for ISOO access to the actual information that is subject to program management is in general hedged in by provisions for appeal, as is any authority for directing action by the agencies.

4. In regard to the responsibilities of the Agency to furnish ISOO access to information, Section 5-405 specifies that agencies shall submit to ISOO "such information or reports as the Director of the Office may find necessary to carry out the Office's responsibilities." Again, the key is necessity to fulfill ISOO responsibilities. The Order provides specifically that agencies submit certain items to ISOO:

a. any designations of "other categories" of information--in addition to the six categories delineated in the Order--that may be considered for classification, as determined by an agency head (Sections 1-301(g) and 1-304);

b. any special procedures for systematic review and declassification of information concerning the identities of clandestine human agents (DCI only, Section 3-403);

c. a copy of any information security regulation or systematic declassification review guideline (Section 5-401);

d. notification of violations of the Order or implementing directives (Section 5-504).

5. In addition, ISOO Directive No. 1 provides specifically that agencies submit certain items to ISOO:

a. requests for any waivers from portion marking requirements (Section I.G.9);

b. declassification guidelines for foreign government information (Section III.C.1.b);

c. requests for any waivers from the 10-year "subsequent review" period after the first systematic declassification review (Section III.C.2.b.(2)).

6. In regard to any authority of the Agency to deny ISOO access to information, Section 4-101 of the Order provides in part that "No person may be given access to classified information unless...access is necessary for the performance of official duties." Section IV.B.1 of ISOO Directive No. 1 provides in part that "Classified information shall be made available to a person only when the possessor of the classified information establishes in each instance...that access is essential to the accomplishment of official Government duties...."

7. In view of the foregoing, the Agency properly may furnish ISOO access to information about our Executive Order 12065 implementation program, but we may provide access to the actual information that is subject to the program only upon an advance showing to our satisfaction that the information is necessary to the performance of ISOO responsibilities. We also must determine in advance that ISOO access does not conflict with the DCI's statutory responsibility to protect Agency information and intelligence sources and methods information (National Security Act of 1947 and CIA Act of 1949).

8. In regard to the specific access request, the 12 April 1979 ISOO letter addressed to the DDA laid out ISOO's schedule for "inspections" of agency programs during the period April through

September 1979. (This letter presumably was sent to each agency's "senior official" designated "to conduct an active oversight program to ensure effective implementation of the Order" (Section 5-404(a))). The letter cited the Director, ISOO's authority (pursuant to Section 5-202(h)) to conduct on-site reviews of the information security program in each agency, and it presented the schedule as "a program of detailed on-site inspections of agency programs." The letter stated in part that ISOO program analysts would, among other things, "devote maximum effort to inspecting actual documents contained in agency holdings to review the propriety of classification, proper marking, over-use of classification beyond 6 years...." The letter requested that the "full extent" of the DDA's authority "be applied to insure that the ISOO analysts are given the necessary cooperation and access to classified information as required to accomplish their duties under this oversight program."

9. Based on the outline of responsibilities in paragraphs 2 thru 7 above, ISOO inspection of Agency documents to review propriety of classification level, duration, and marking is a legitimate oversight function. However, such inspection must be accomplished in a manner consistent with our statutory responsibilities to protect information from disclosure. Although the Order provides that the DCI may formally deny access to information (subject to appeal), it would be preferable to reach agreement with ISOO, in advance of any inspection, on ground rules that will properly balance ISOO responsibilities and our security concerns. When we spoke to the Director, ISOO on 19 April 1979, he took a cooperative approach to the access question, stating he realized there were certain areas of Agency information to which ISOO personnel should not have access for "inspection" purposes. Accordingly, the following three options for handling access by ISOO personnel are presented, followed by a brief discussion and recommendation.

Option 1 - Staff-like Access:

a. Staff-like access would require staff-type security clearances, including reinvestigation-level polygraph examination.

b. The office sponsoring (or responsible for) the inspection team would request and justify such clearances.

c. The Office of Security would do a file review on the clearances the individuals now hold to see if they are adequate under DCID 1/14 standards.

SUBJECT: Executive Order 12065: Access by the Information Security Oversight Office to CIA Information

d. When OS conducts such a full investigation and grants staff-type clearances, the cleared individuals may be authorized to be issued ~~receive~~ a badge; but this would depend on other factors such as frequency of visits.

Option 2 - Memorandum of Understanding

a. A Memorandum of Understanding between the DCI and the Director, ISOO, would specify ISOO areas of interest.

b. The MOU also would specify agreed procedures covering: pre-screening information, providing access to information determined to be "relevant" to the specified ISOO areas of interest, and withholding or deleting information that is not "relevant" or that reveals intelligence sources and methods; review of inspector's notes for proper classification; requirements for handling and storage of any Agency classified information taken off premises; and other appropriate details.

c. If the procedures specified in the MOU were followed, the ISOO personnel's normal GSA clearances, SCI clearances, and Agency liaison clearances would suffice.

Option 3 - Agreed Procedures

a. Draft procedures would be prepared, covering access to Agency information in the possession of other agencies as well as in our possession, and providing for pre-screening and for withholding or sanitizing where appropriate.

b. The procedures would not specify ISOO areas of interest in detail, but rather provide for this to be determined in the context of each visit. Other matters would be covered as in Option 2.

c. The procedures would be agreed to informally by the AI/DDA and D/ISOO, and coordinated within the Agency by the AI/DDA.

d. The final agreed procedures would be sent to D/ISOO under a letter from the DDA and serve as the basis for any ISOO access.

e. The normal GSA clearances, SCI clearances, and Agency liaison clearances would suffice.

SUBJECT: Executive Order 12065: Access by the Information Security Oversight Office to CIA Information

10. It is recommended that we pursue Option 3. Staff-like access (Option 1) is not necessary in view of ISOO responsibilities and frequency of visits. A Memorandum of Understanding (Option 2) would be too formal and inflexible in view of our Executive Branch relationship with ISOO and the difficulty of specifying ISOO areas of interest in advance, in terms of specific subject matter.

11. An initial draft of ISOO access procedures is attached.

[redacted]

STATINTL

Attachment

CONCUR:

_____
Office of Security

_____
Office of General Counsel

_____
Directorate of Administration

Distribution:
Original - AI/DDA (Return to RAB for ISOO file)
1 - AI/DDA
1 - OGC
1 - OS
1 - IPS
1 - ISAS/CRG
1 - RAB (hold)